



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/987,911	11/16/2001	Mark Crosbie	10012198	7932

7590 02/14/2008
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

ABRISHAMKAR, KAVEH

ART UNIT	PAPER NUMBER
----------	--------------

2131

MAIL DATE	DELIVERY MODE
-----------	---------------

02/14/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

AR

Office Action Summary	Application No. 09/987,911	Applicant(s) CROSBIE ET AL.	
	Examiner KAVEH ABRISHAMKAR	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 November 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-6 and 14-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6, and 14-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on November 1, 2007 has been entered.

1. Claims 1-6, and 13-24 are currently pending consideration.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-6, and 13-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ko (U.S. Patent 7,024,694) in view of Moran (U.S. Patent 6,647,400).

Regarding claim 1, Ko discloses:

reading an event representing at least one system call (Figure 4, step 414, column 5, lines 49-54: "upon detecting an event"), wherein the event is a kernel audit

Art Unit: 2131

record read from an intrusion detection data source (IDDS) (column 5, lines 20-24),
wherein loadable kernel module is inserted into the kernel;

routing an event to a template, the event comprising multiple parameters and the template comprising a sequence of connected logic nodes comprising at least one input node, at least one filter node, and at least one output node (column 4, lines 45-60),
wherein if a specific criteria is detected, the event is routed and the system call is examined for one of multiple parameters;

filtering the event, based on the sequence of logic nodes of the template, as a possible intrusion based on the multiple parameters and either dropping the event or outputting the event (column 5, lines 29-46), *wherein the recorded target attributes are filtered, and then the system examines the log for intrusion detection purposes*

the filtering comprising:

determining a filename based on the event (column 4, lines 49-60), *wherein a number of parameters related to the file can be used as the target attribute;*

outputting the event for each event indicating modification of a critical file based upon the determined filename (column 4, lines 49-60), *wherein a number of parameters related to the file can be used as the target attribute and these target attributes are examined for intrusion detection purposes.*

Ko does not explicitly disclose creating an intrusion alert for each event output from said filtering. Moran discloses examining events and then using an IDS to assign an alert (Moran: column 8, lines 30-35). The system of Ko can be used with "any type of intrusion detection mechanism" (Ko: column 5, lines 42-45). Ko and Moran are

Art Unit: 2131

analogous arts because both have to do with detecting intrusions. It would have been obvious to one of ordinary skill in the art at the time of invention to use the system of Moran to issue alerts so that the operator can respond in time to avert damage to the computer files (Moran: column 3, lines 1-2).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Ko discloses:

The method of claim 1, wherein said filtering further comprises providing the event to the determining a filename for each event comprising a parameter indicating modification of a permission bit on a file or directory (Ko: column 4, lines 49-60), *wherein the target attribute (filtering) can be any parameter related to a file involved in a system call including a permission mode.*

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Ko discloses:

The method of claim 1, wherein said filtering further comprises providing the event to the determining a filename for each event comprising a parameter indicating opening a file for truncation (Ko: column 4, lines 49-60), *wherein the target attribute which is used for filtering can include any parameter related to a file involved in a system call including opening a file for truncation.*

Art Unit: 2131

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Ko discloses:

The method of claim 1, wherein said filtering further comprises providing the event to the determining a filename for each event comprising a parameter indicating modification of the ownership or group ownership of a file (Ko: column 4, lines 49-55), *wherein the target attribute used in filtering can be a group ID or an owner user ID.*

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Ko discloses:

The method of claim 1, further comprising an alert message for each renamed file including the filename of the file and the new filename of the file (column 4, lines 49-60), *wherein the target attribute used in filtering can be any parameter related to a file involved in the system call including a filename.*

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Ko discloses:

The method of claim 1, comprising configuring a template based on a list of files and directories to be included or excluded based on whether the files and directories are considered unmodifiable (Ko: column 5, lines 56-61), *wherein only selective target attributes are recorded based on the event.*

Art Unit: 2131

Claim 13 is rejected as applied above in rejecting claim 1. Furthermore, Ko discloses:

A computer-readable medium storing instructions which, when executed by a processor, cause the processor to implement the method steps of claim 1 (Ko: column 3, lines 17-21), wherein *the code is typically stored on a computer-readable medium.*

Regarding claim 14, Ko discloses:

a processor (column 3, lines 32-35);

a memory storing instructions which, when executed by the processor, cause the processor to:

read an event from an intrusion detection data source (IDDS) (Figure 4, step 414, column 5, lines 49-54: "upon detecting an event"), wherein the event is a kernel audit record (column 5, lines 20-24), *wherein loadable kernel module is inserted into the kernel;*

route events to a template, wherein the event comprises one or more parameters and the template comprises a sequence of connected logic nodes comprises at least one input node, at least one filter node, and at least one output node (column 4, lines 45-60), *wherein if a specific criteria is detected, the event is routed and the system call is examined for one of multiple parameters;*

filter the event, based on the template, as a possible intrusion based on one of the one or more parameters and either dropping the event or outputting the event (column 4, lines 49-60), *wherein a number of parameters related to the file can be used*

Art Unit: 2131

as the target attribute and these target attributes are examined for intrusion detection purposes.

Ko does not explicitly disclose creating an intrusion alert for each event output from said filtering. Moran discloses examining events and then using an IDS to assign an alert (Moran: column 8, lines 30-35). The system of Ko can be used with "any type of intrusion detection mechanism" (Ko: column 5, lines 42-45). Ko and Moran are analogous arts because both have to do with detecting intrusions. It would have been obvious to one of ordinary skill in the art at the time of invention to use the system of Moran to issue alerts so that the operator can respond in time to avert damage to the computer files (Moran: column 3, lines 1-2).

Claim 15 is rejected as applied above in rejecting claim 20. Furthermore, Ko discloses:

The system of claim 20, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to provide the event to the determine a filename instructions for each event comprising one of the one or more parameters indicating modification of the permission bits on a file or directory (Ko: column 4, lines 49-60), *wherein the target attribute (filtering) can be any parameter related to a file involved in a system call including a permission mode.*

Claim 16 is rejected as applied above in rejecting claim 20. Furthermore, Ko discloses:

Art Unit: 2131

The system of claim 20, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to provide the event to the determine a filename instructions for each event comprising one of the one or more parameters indicating that a file was opened for truncation (Ko: column 4, lines 49-60), *wherein the target attribute which is used for filtering can include any parameter related to a file involved in a system call including opening a file for truncation.*

Claim 17 is rejected as applied above in rejecting claim 20. Furthermore, Ko discloses:

The system of claim 20, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to provide the event to the determine a filename instructions for each event comprising one of the one or more parameters indicating modification of the ownership or group ownership of a file (Ko: column 4, lines 49-55), *wherein the target attribute used in filtering can be a group ID or an owner user ID.*

Claim 18 is rejected as applied above in rejecting claim 20. Furthermore, Ko discloses:

The system of claim 20, wherein the instructions further comprise instructions causing the processor to output an alert message for each renamed file, the alert message comprising the filename of the file and the filename of the renamed file

Art Unit: 2131

(column 4, lines 49-60), *wherein the target attribute used in filtering can be any parameter related to a file involved in the system call including a filename.*

Claim 19 is rejected as applied above in rejecting claim 20. Furthermore, Ko discloses:

The system of claim 20, wherein the instructions causing the processor to configure a template based on a list of files and directories to be included or excluded based on whether the files and directories are considered unmodifiable (Ko: column 5, lines 56-61), *wherein only selective target attributes are recorded based on the event.*

Claim 20 is rejected as applied above in rejecting claim 14. Furthermore, Ko discloses:

The system of claim 14, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to determine the filename based on the event and output the event for each event indicating modification of critical file based upon the determined filename (Ko: column 4, lines 49-60), *wherein the target attribute used in filtering can be any parameter related to a file involved in the system call including a filename.*

Claim 21 is rejected as applied above in rejecting claim 1. Furthermore, Ko discloses:

The method of claim 1, wherein said filtering further comprises determining a subdirectory of a directory based on the event and outputting the event for each event indicating modification to the determined subdirectory (Ko: column 4, lines 48-55), *wherein a pathname (including a subdirectory) can be a target attribute which is used in filtering.*

Claim 22 is rejected as applied above in rejecting claim 14. Furthermore, Ko discloses:

The system of claim 14, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to determine a subdirectory of a directory based on the event and output the event for each event indicating modification to a predetermined subdirectory of a directory (Ko: column 4, lines 48-55), *wherein a pathname (including a subdirectory) can be a target attribute which is used in filtering.*

Claim 23 is rejected as applied above in rejecting claim 1. Furthermore, Ko discloses:

The method of claim 1, wherein said reading an event comprises reading an event from an event-driven correlation service of the IDDS Figure 4, step 414, column 5, lines 49-54: "upon detecting an event").

Claim 24 is rejected as applied above in rejecting claim 14. Furthermore, Ko discloses:

The system of claim 14, wherein the instructions causing the processor to read an event comprise instructions causing the processor to read an event from an event-driven correlation service of the IDDS Figure 4, step 414, column 5, lines 49-54: "upon detecting an event").


Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


Kaveh Abrishamkar
AU 2131

KA
K.A. 2/12/08
02/12/08